日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　６月１１日

出願番号
Application Number: 特願２００１－１７４９８１

出願人
Applicant(s): 株式会社日立製作所

２００１年１１月２６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３１０２４００

【書類名】　特許願

【整理番号】　K01001231A

【あて先】　特許庁長官

【国際特許分類】　G06F 17/60

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　吉川　達也

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　鮫嶋　茂稔

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　河野　克己

【発明者】

【住所又は居所】　東京都千代田区神田駿河台四丁目６番地　株式会社日立製作所　情報制御システム事業部内

【氏名】　中野　利彦

【発明者】

【住所又は居所】　茨城県ひたちなか市市毛１０７０番地　株式会社日立製作所　ビルシステムグループ内

【氏名】　小林　延久

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　分散システムにおけるサービス提供方法

【特許請求の範囲】

【請求項１】

所定のサービスを提供するための情報処理を実行するサービスデバイスと、前記サービスデバイスに対して前記サービスの要求を示す要求情報を送信する要求デバイスとからなる分散システムにおいて、

前記サービスデバイスが、前記要求デバイスから送信される前記要求情報を受信するステップと、

前記サービスデバイスが、当該サービスデバイスの所定範囲内の状況を示す周辺情報を収集するステップと、

前記サービスデバイスが、前記周辺情報に基づいて、前記要求情報で要求されるサービスを提供可能な場合は、提供可能な前記サービスを提供するための情報処理を実行するステップとを有することを特徴とする分散システムにおけるサービス提供方法。

【請求項２】

請求項１に記載の分散システムにおけるサービス提供方法において、

前記周辺情報には、前記サービスデバイスおよび前記要求デバイスの少なくとも一方から所定範囲内に、予め定められた周辺デバイスが存在するか否か示す情報が含まれ、

前記情報処理を実行するステップでは、前記周辺デバイスが前記所定範囲内に存在する場合に、前記情報処理を実行することを特徴とする分散システムにおけるサービス提供方法。

【請求項３】

請求項２に記載の分散システムにおけるサービス提供方法において、

前記周辺デバイスは、前記サービスを受ける権限を有することを示す識別情報を記憶することを特徴とする分散システムにおけるサービス提供方法。

【請求項４】

請求項１乃至３のいずれかに記載の分散システムにおけるサービス提供方法に

おいて、

前記サービスデバイスは、サービス毎に当該サービスを提供する場合の条件を対応付けた拡張アクセスコントロールリストを記憶する記憶装置と接続し、

前記情報処理を実行するステップは、収集された前記周辺情報が前記条件に対応する場合に、前記情報処理を実行することを特徴とする分散システムにおけるサービス提供システム。

【請求項５】

請求項４に記載の分散システムにおけるサービス提供方法において、

前記拡張アクセスコントロールリストには、前記条件が、前記周辺情報に応じて、前記サービスを受けることが可能な利用者もしくは要求デバイスを変更されて格納されることを特徴とする分散システムにおけるサービス提供方法。

【請求項６】

請求項１乃至５のいずれかに記載の分散システムにおけるサービス提供方法において、

前記サービスを提供するための情報処理には、前記要求デバイスから前記サービスデバイスへのアクセスが含まれることを特徴とする分散システムにおけるサービス提供方法。

【請求項７】

所定のサービスを提供するための情報処理を実行するサービス提供装置において、

前記サービスの要求を示す要求情報を送信する要求デバイスから前記要求情報を受信する受信装置と、

前記受信装置と接続され、記憶装置に格納されたプログラムに従って、当該サービス提供装置の所定範囲内の状況を示す周辺情報を収集し、前記周辺情報に基づいて、前記要求情報で要求されるサービスを提供可能な場合は、提供可能な前記サービスを提供するための情報処理を実行する処理装置とを有することを特徴とするサービス提供装置。

【請求項８】

請求項７に記載のサービス提供装置において、

前記周辺情報には、前記サービスデバイスおよび前記要求デバイスの少なくとも一方から所定範囲内に、予め定められた周辺デバイスが存在するか否か示す情報が含まれ、

前記処理装置は、前記周辺デバイスが前記所定範囲内に存在する場合に、前記情報処理を実行することを特徴とするサービス提供装置。

【請求項９】

請求項８に記載のサービス提供装置において、

前記周辺デバイスは、前記サービスを受ける権限を有することを示す識別情報を記憶することを特徴とするサービス提供装置。

【請求項１０】

請求項７乃至９のいずれかに記載のサービス提供装置において、

サービス毎に当該サービスを提供する場合の条件を対応付けた拡張アクセスコントロールリストを記憶する記憶装置をさらに有し、

前記処理装置は、収集された前記周辺情報が前記条件に対応する場合に、前記情報処理を実行することを特徴とするサービス提供装置。

【請求項１１】

請求項１０に記載のサービス提供装置において、

前記処理装置は、前記記憶装置に、前記条件を、前記周辺情報に応じて、前記サービスを受けることが可能な利用者もしくは要求デバイスを変更して格納することを特徴とするサービス提供装置。

【請求項１２】

請求項７乃至１１のいずれかに記載のサービス提供装置において、

前記サービスを提供するための情報処理には、前記要求デバイスから前記サービスデバイスへのアクセスが含まれることを特徴とするサービス提供装置。

【請求項１３】

所定の領域への人間の入場を管理する入場管理システムにおいて、

前記領域への入場を物理的に制限する制限装置と、

前記制限装置と接続する手段と、前記制限手段を開放する開放要求を、要求装置から受信する手段と、所定範囲内に、前記領域への入場が許可される個人また

は組織を識別する情報が格納された周辺装置が存在するかを検知する手段と、前記周辺装置が存在する場合に、前記制限装置に対し、前記領域への入場を許容する制御を実行する手段とを有する制御装置と

を備えたことを特徴とする入場管理システム。

【請求項１４】

請求項１３に記載の入場管理システムにおいて、

前記制限装置は、錠を備えたドアであり、

前記制御装置は、前記周辺装置が存在する場合に、前記錠を開錠するよう制御することを特徴とする入場管理システム。

【請求項１５】

請求項１３または１４のいずれかに記載の入場管理システムにおいて、

前記検知する手段は、前記所定範囲に所定の信号を無線で発信し、発信された無線に対する応答に応じて、検知することを特徴とする入場管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、所定の機能を実行するデバイスの制御に関するものである。この中でも、アクセスコントロールリスト(ACL)などの情報を用いて各デバイスをアクセス制御する方式のセキュリティ分野を対象としている。また、さらに、入退出管理や盗難防止、物品管理等において適用可能な技術に関する。

【０００２】

【従来の技術】

従来、デバイスが複数存在する分散システムにおけるアクセス制御方法として、例えば特開２０００－１１２８９１号公報に記載されている方法がある。これによると、システム内の各デバイスに分散アクセスコントロールリスト(ACL)を個別に持たせることによって、ユーザ属性に応じたアクセス制御を行っていた。また、設定対象の計算機にその都度ログインすることなしに当該設定を可能とすることで、設定の手間を軽減し設定ミスを防止していた。

【０００３】

【発明が解決しようとする課題】

上記従来技術においては、様々なユーザが訪問するオフィスビル等において、制限区域内に重要物が存在する場合には入室を禁止し、そうでない場合は許可するような場面を想定した時、従来の画一的なアクセス制御では運用/管理者のアクセスレベルの設定変更作業やユーザの設定変更要求からの時間的な遅れという点で限界があった。

【０００４】

本発明は、分散システムにおいてユーザ及びサービスデバイスの状況に応じて、より柔軟なアクセス制御を実現することを目的とする。

【０００５】

【課題を解決するための手段】

上記目的を達成するために、本発明は、デバイスの周辺情報に応じて、アクセス制御を含むサービス提供のための情報処理を行うものである。周辺情報は、デバイスの所定範囲内の状況を示す情報であり、サービス提供の条件となるものである。周辺情報には、所定デバイスから所定の範囲内にある他のデバイスの状態を示す情報が含まれる。他のデバイスの状態には、他のデバイス（予め定められた）が存在するか否か、他のデバイスの運転状況が含まれる。また、周辺情報には、デバイスから所定範囲内に、サービスを受ける者が存在するか、またその者がサービスを受ける権利を有する者かを示す情報が含まれる。

【０００６】

本発明には、所定のサービスを提供するサービスデバイスから所定範囲内に、サービスを要求する要求デバイスと、サービスデバイスもしくは要求デバイスから所定範囲内に、要求デバイスにサービスを受ける権限を与える周辺デバイスが存在するか否かに従って、サービスデバイスが所定のサービスを提供するかどうかを制御する。サービスデバイスが入出場を制御するドア等で、要求デバイスが携帯電話で、周辺デバイスが電子的に個人または組織を識別する情報が格納されたＩＤカードである場合の例を説明する。この例では、所定の部屋に入場するためにドアの鍵を開ける指示を、携帯電話からドアに送信する。ドアの鍵の開閉を制御する制御装置は、指示を受付けるとドアもしくは携帯電話から所定範囲内に

、当該部屋への入場が許可される個人を識別するＩＤカードが存在すれば、携帯電話からの要求に対応してドアの鍵を開ける。ＩＤカードの存在は、制御装置から電波を発して行ってもよい。

【０００７】

また、本発明には、サービスデバイスへアクセス可能なデバイス（サービスを受けることが可能な利用者）を、周辺情報に応じて、に変えることも含まれる。

【０００８】

【発明の実施の形態】

以下、本発明の実施例を図１により説明する。

図１は、本発明におけるアクセス制御システムの適用形態例を示す。主な構成要素としては、サービスデバイス（電子錠）０１１４に対してサービスを要求するユーザ０１１０、ユーザインタフェースを提供する携帯端末０１１１、携帯端末０１１１の周辺に存在する同伴者０１１２が所有するユーザ周辺デバイス（IDカード、携帯端末等）０１１３、ユーザの要求するサービスを提供するサービスデバイス（電子錠）０１１４、サービスデバイス（電子錠）０１１４の周辺に存在する不審者０１１５が所有する機器周辺デバイス（未登録IDカード、携帯端末等）０１１６等からなる。

【０００９】

図２は、本発明におけるアクセス制御システムの構成図である。主な構成要素としてユーザ０２１０、携帯端末０２１１、サービスデバイス０２２０、ユーザ周辺デバイス０２１８、機器周辺デバイス０２２８から構成される。このシステムは環境中に複数デバイスが分散して存在し、各サービスデバイス０２２０のハードディスク領域には拡張アクセスコントロールリスト(Extended Access Control List:EACL)０２２３が格納され、共通通信プロトコルを用いた無線通信モジュール(所定の通信技術を用いることができる)を有する。ユーザ０２１０は携帯端末０２１１(携帯電話/PDA等)を介して必要なサービスを要求し、サービスデバイス０２２０よりサービスを受信する。ユーザ０２１０は携帯端末０２１１を用いて、個人認証情報（ユーザID：676001027、グループID：105u）/サービス情報（要求サービスID：応接室開錠）をサービスデバイスに対して送信する。

【００１０】

ただし、個人認証情報は携帯端末０２１１に記憶、サービス情報はネットワーク経由で入手したサービス一覧より選択する。携帯端末０２１１上の周辺デバイス検知処理０２１６は、携帯端末０２１１上の通信処理０２１７に対して周辺デバイス検索信号を送信する。通信管理処理０２１７は、周辺デバイスに対してデバイス情報配信要求信号を同報配信する。無線通信内に存在するユーザ周辺デバイス０２１８はデバイス情報配信要求信号を受信すると、通信処理０２１９によって周辺デバイス固有のグローバルユニークなID（周辺デバイスID：F0032A8）や周辺デバイスの状態（稼動中、スリープ等）を携帯端末上の通信処理０２１７に対して送信する。周辺デバイス情報を受信した通信処理０２１７は、周辺デバイス検知処理０２１６に情報を配信する。周辺デバイス情報を受信した周辺デバイス検出処理０２１６は、ユーザ周辺デバイス情報DB０２１４内のテーブルに周辺デバイス情報を書き込む。

【００１１】

さらに、周辺デバイス検出処理０２１６はユーザ０２１０から最初に送信された個人認証情報/要求サービス情報に周辺デバイス情報を併せて、サービスデバイス０２２０に送信する。周辺デバイス検出処理０２１６は常時起動しており、一定周期でユーザ周辺デバイス０２１８の検出を行う。ユーザ情報/ユーザ周辺情報を受信したサービスデバイス０２２０上のアクセス制御処理０２２２は、サービスデバイス０２２０の周辺デバイス０２１３の情報収集を自身の機器周辺デバイス検出処理０２２５に対して要求する。要求を受信した機器周辺デバイス検出処理０２２５は、前記の携帯端末０２１１上のユーザ周辺デバイス検出処理０２１６と同様の処理によって、機器周辺デバイス０２２８の情報を獲得する。併せて、周辺デバイス情報DB０２２６内のテーブルに獲得した周辺デバイス情報を書き込む。機器周辺デバイス検出処理０２２５は、獲得した周辺デバイス情報をアクセス制御処理０２２２に配信する。

【００１２】

周辺デバイス情報を受信したアクセス制御処理０２２２は、サービスデバイス０２２０上に記憶されたEACL０２２３を参照する。その際、携帯端末０２１１か

ら受信したユーザ情報/ユーザ周辺情報及び前記のサービスデバイス周辺情報を利用する。アクセス制御処理０２２２は、受信した情報（ユーザID、グループID、要求サービスID、ユーザ周辺デバイス情報、機器周辺デバイス情報）とEACL０２２３を照合することによって、アクセスレベルを決定する。但し、ユーザ０２１０やユーザ周辺デバイス０２１８の履歴情報０２３０を参照してアクセスレベルを決定する場合もある。その際は、EACL０２２３を参照して決定されたアクセスレベルと比較を行い、ある政策（例えば、アクセスレベルの低い方を採用する等）に従ってアクセスレベルを決定する。アクセス制御処理０２２２は決定されたアクセスレベルのモードでサービスデバイス０２１２を制御し、ユーザ０２１０にサービスを提供する。その際の情報/サービスの流れについては、図３から図９で詳述する。

【００１３】

尚、サービスデバイス０２２０は、ユーザ０２１０からのサービス要求時のみならず、上記ユーザ個人情報及びユーザ周辺情報を任意のタイミングで送信要求することが可能であることを付記する。

【００１４】

図３は、本発明におけるシステム全体の処理を示すフローチャートである。ＳＴ０３１０において、ユーザ０２１０は携帯端末０２１１を介してサービスデバイス０２２０に対してサービスを要求する。その際、ユーザ０２１０は携帯端末０２１１を介して明示的にユーザID、グループID及び要求サービスIDを入力するか、携帯端末０２１１に予め記憶された各項目を選択しサービスデバイス０２２０に対してメッセージを送信する。ＳＴ０３１１においては、ユーザ情報のメッセージ送信要求を受けた携帯端末０２１１はユーザ周辺デバイス０２１８の検索を開始する。携帯端末０２１１は、ユーザ周辺デバイス０２１８よりデバイス情報を受信する。

【００１５】

また、他に周辺デバイスが存在しないかどうかチェックを行い、ユーザ周辺デバイス０２１８が存在すれば処理を繰り返す。ユーザ周辺デバイス０２１８が存在しなければ、ＳＴ０３１２に進む。ＳＴ０３１２においては、ユーザ０２１０

から入力あるいは携帯端末０２１１上に記憶されたユーザID、グループID、要求サービスIDと、ＳＴ０３１１で獲得したユーザ周辺デバイス情報を併せて、サービスデバイス０２２０に送信する。

【００１６】

ＳＴ０３１３においては、携帯端末０２１１からサービス要求メッセージを受信すると、機器周辺デバイス０２２８の探索を開始する。サービスデバイス０２２０は、機器周辺デバイス０２２８よりデバイス情報を受信する。また、他に周辺デバイスが存在しないかどうかチェックを行い、機器周辺デバイス０２２８が存在すれば処理を繰り返す。機器周辺デバイス０２２８が存在しなければ、ＳＴ０３１４に進む。ＳＴ０３１４においては、携帯端末０２１１より受信した情報とＳＴ０３１３で獲得した機器周辺デバイス情報を利用してEACLの参照を行い、アクセスレベルを決定する。ＳＴ０３１５においては、ＳＴ０３１４で決定したアクセスレベルに基づいてユーザ０２１０に対してサービスを提供する。

【００１７】

図２７は、本発明における履歴情報データベースを用いた場合のシステム全体の処理を示すフローチャートである。ＳＴ２７１０乃至ＳＴ２７１４においては、ＳＴ０３１０乃至ＳＴ０３１４と同一の処理を行う。ＳＴ２７１５は、履歴情報ＤＢ０２３０を参照してアクセスレベルを決定する。決定したアクセスレベルとＳＴ２７１４で決定されたアクセスレベルをある政策（例えば、アクセスレベルの低い方を選択する等）に従ってアクセスレベルを決定する。ＳＴ２７１６においては、ＳＴ２７１５で決定したアクセスレベルに基づいてユーザ０２１０に対してサービスを提供する。

【００１８】

図４は、本発明における携帯端末上の周辺デバイス検出処理を示すフローチャートである。ＳＴ０４１０において、ユーザ０２１０からＩ／Ｏ０２１２、アプリケーション０２１３を介してユーザ情報及びサービス要求を受信する。ＳＴ０４１１においては、通信処理０２１７に対して周辺デバイス検索要求を送信する。具体的には、各デバイスに対して同報メッセージを送信する要求を出す。ＳＴ０４１２においては、ユーザ周辺デバイス０２１８から通信処理０２１７へ送信

された周辺デバイス情報を受信する。ＳＴ０４１３においては、機器構成管理処理０２１５にユーザ周辺デバイス０２１８の情報取得要求を送信する。ＳＴ０４１４においては、ユーザ情報及び機器構成管理処理０２１５から受信した情報をサービスデバイス０２２０に送信する。

【００１９】

図５は、本発明における携帯端末上の機器構成管理処理を示すフローチャートである（非常駐処理）。ＳＴ０５１０において、周辺デバイス検出処理０２１６からユーザ周辺デバイス情報データベース０２１４への参照要求を受信する。ＳＴ０５１１においては、ユーザ周辺デバイス情報を元にユーザ周辺デバイス情報データベース０２１４を参照する。ＳＴ０５１２においては、ＳＴ０５１１で得られた参照結果を周辺デバイス検出処理０２１６に送信する。

【００２０】

図６は、本発明における携帯端末上の機器構成管理処理を示すフローチャートである（常駐処理）。ＳＴ０６１０において、通信処理０２１７からユーザ周辺デバイス情報を受信する。ＳＴ０６１１において、ユーザ周辺機器情報を元にユーザ周辺デバイス情報データベース０２１４を参照する。ＳＴ０６１２においては、周辺デバイス検出処理０２１６にユーザ周辺デバイス０２１８の状態変更を通知する。次に、ＳＴ０６１０に戻る。

【００２１】

図７は、本発明におけるサービスデバイス上の周辺デバイス検出処理を示すフローチャートである。ＳＴ０７１０において、携帯端末０２１１からサービス要求を受信する。ＳＴ０７１１においては、通信処理０２２７に対して周辺デバイス検索要求を送信する。具体的には、各デバイスに対して同報メッセージを送信する要求を出す。ＳＴ０７１２においては、機器周辺デバイス０２２８から通信処理０２２７へ送信された周辺デバイス情報を受信する。ＳＴ０７１３においては、機器構成管理処理０２２５に機器周辺デバイス０２２８の情報取得要求を送信する。ＳＴ０７１４においては、ユーザ情報及び機器構成管理処理０２２５から受信した情報をアクセス制御処理０２２２に送信する。

【００２２】

図８は、本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである（非常駐処理）。ＳＴ０８１０において、周辺デバイス検出処理０２２４から機器周辺デバイス情報データベース０２２６への参照要求を受信する。ＳＴ０８１１においては、機器周辺デバイス情報を元に機器周辺デバイス情報データベース０２２６を参照する。ＳＴ０８１２においては、ＳＴ０８１１で得られた参照結果を周辺デバイス検出処理０２２４に送信する。

【００２３】

図９は、本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである（常駐処理）。ＳＴ０９１０において、通信処理０２２７から機器周辺デバイス情報を受信する。ＳＴ０９１１において、機器周辺機器情報を元に機器周辺デバイス情報データベース０２２６を参照する。ＳＴ０９１２においては、アクセス制御処理０２２２に機器周辺デバイス０２２８の状態変更を通知する。次に、ＳＴ０９１０に戻る。

【００２４】

図１０は、本発明においてユーザが携帯端末を介してサービスを要求する際に送信するメッセージを示した図である。上記メッセージは、通信ヘッダ１０１０及びデータ１０１４からなり、その主な構成要素としては、ユーザの個人認証に用いられるユーザID１０１１、ユーザが属するグループID１０１２、ユーザがサービスデバイスに対して要求する要求サービス１０１３等からなる。また、データ１０１４の主な構成要素としては、ユーザ周辺デバイスに関する周辺機器構成１０１５、要求サービス１０１６等からなる。

【００２５】

図１１は、本発明におけるユーザから送信の情報を示す図である。主な構成要素としては、ユーザからデータが送信された時間を表すデータ送信日時１１１０、ユーザ個人を特定するユーザID１１１１、ユーザが属するグループID１１１２、ユーザ０２１０がサービスデバイス０２２０に対して要求する要求サービスID１１１３等からなる。

【００２６】

図１２は、本発明におけるユーザ周辺デバイス情報を示す図である。主な構成

要素としては、周辺を検索してデータが得られた時間を表すデータ受信日時１２１０、ユーザ周辺に存在するユーザ周辺デバイス情報１２１１等（ID、状態値等）からなる。但し、ユーザ周辺デバイス情報１２１１は、ユーザ周辺デバイス０２１８が存在した場合のみ有効である。

【００２７】

図１３は、本発明における周辺デバイス情報を利用したEACLを示す図である。主な構成要素として、ユーザが本EACLを有するサービスデバイスに対して許可されるアクセスレベル１３１０、ユーザの属するグループID１３１１、ユーザ周辺に存在する機器のユーザ周辺デバイス情報（ID、状態値等）１３１２、サービスデバイス周辺に存在する機器周辺デバイス情報（ID、状態値等）１３１３からなる。但し、ユーザ周辺情報１３１２及び機器周辺デバイス情報１３１３は、ユーザ周辺デバイス０２１８及び機器周辺デバイス０２２８が存在した場合のみ有効である。

【００２８】

図２３は、本発明におけるサービス要求／提供時の時間（帯）によってアクセスレベルが変化するEACLを示す図である。主な構成要素として、受信情報２３１０、時間（帯）２３１１、アクセスレベル２３１２等から構成される。受信情報２３１０は、上記ユーザから受信したグループID１３１１、ユーザ周辺デバイス情報（ID、状態値等）１３１２、上記サービスデバイス周辺に存在する機器周辺デバイス情報（ID、状態値等）１３１３からなる。時間（帯）は、サービス要求あるいはサービス提供時のある時刻あるいはある時間帯を示す。アクセスレベル３１２は、上記アクセスレベル１３１０と同値である。同一の情報を受信した場合でも、サービス要求／提供時刻によって異なったアクセスレベルを提供するものである。

【００２９】

図１４は、本発明におけるアクセスレベルと実行許可処理との関係を示す図である。主な構成要素として、上記アクセス制御処理において決定されたアクセスレベル１４１０、サービスデバイスで実行され得る実行処理１４１１、各アクセスレベルにおける実行処理を行うか行わないかを示したアクセス権限１４１２等

からなる。

【００３０】

図１５は、本発明における周辺デバイスの判定基準を示す図である。携帯端末０２１１やサービスデバイス０２１２のように周辺デバイス検出処理０２１４を備えたデバイスi１５１４を中心とした半径d_L１５１１の円を想定する。ここで、d_Lはデバイス固有の近傍距離閾値である。このとき、その円周を近傍境界線１５１０として、デバイスi１５１４と周辺デバイスj１５１３、非周辺デバイスk１５１５間の距離を赤外線近接センサ等を用いて測定する。デバイスi１５１４と周辺デバイスj、非周辺デバイスkとの距離をそれぞれd_{ij}１５１２、d_{ik}１５１２とする。このとき、不等式１５１６を用いて対象とするデバイスが、デバイスi１５１４の周辺デバイスj１５１３であるか、あるいは非周辺デバイスk１５１５であるかを判定する。

【００３１】

図１６は、本発明における周辺閾値（近傍距離閾値）を既定方法を示す図である。主な構成要素としては、ユーザ１６１０、ユーザ周辺デバイス１６１１、サービスデバイス１６１２、周辺閾値情報１６１３、ユーザ情報１６１４、周辺閾値１６１５等からなる。ユーザ１６１０は、携帯端末０２１１を通じてユーザ情報１６１４（ユーザID、グループID、要求サービスID等）をサービスデバイス１６１２に送信する。上記ユーザ情報１６１４を受信したサービスデバイス１６１２は、周辺閾値情報DBの参照を行い周辺閾値１６１５を決定する。

【００３２】

その際、利用する情報は、上記ユーザ情報１６１４及びサービスデバイス１６１２情報である。決定された周辺閾値１６１５は、ユーザの所有する携帯端末１６１０に送信される。携帯端末１６１０は、受信した周辺閾値１６１５内を検索範囲１６１６としてユーザ周辺デバイス１６１１の探索を行う。但し、ユーザ周辺デバイス１６１１が同時にサービスデバイス１６１２の周辺デバイスと認識される場合は、ある政策（例えば、アクセスレベルが下がる方の周辺デバイスと認識する等）に従って処理を行う。

【００３３】

図１７は、本発明におけるサービスによる異なる周辺距離の例を示す概略図である。主な構成要素としては、サービス１７１０、周辺距離１７１１等からなる。サービスデバイス０２２０の提供するサービスに応じて、ユーザ０２１０が探索すべき周辺距離１７１１（周辺円領域の半径）を規定する。例えば、「ドアの開錠」サービスに対する周辺距離は、「１０m」、「ドアの施錠」サービスに対する周辺距離は、「０m」等である。

【００３４】

図１８は、本発明におけるアクセス制御方法を適用した実施例１を示す概略図である。主な構成要素として、部長１８１０、課長１８１１、制限区域（金庫）１８１２、不審者１８１３等から構成される。課長１８１１は、携帯端末０２１１としてPDAを所有している。また、部長１８１０はユーザ周辺デバイス０２１８として、自身の情報を登録したIDカードを所有している。また、この適用例のサービスデバイス０２２０としては、金庫の電子錠１８１２を想定している。また、機器周辺デバイス０２２８としては、不審者１８１３が所持する未登録品（IDカード等）を考える。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『課長１８１１一人では開錠禁止の金庫１８１２であるが、部長１８１０同伴の場合は開錠が許可される。ただし、金庫１８１２付近に不審者１８１３が検知された場合開錠されない。』さらに詳述すると、以下のようである。

【００３５】

１．課長１８１１はPDAを用いて、個人認証情報（ユーザID：usr_676001027、グループID：grp_105）/サービス情報（要求サービスID：金庫開錠）１８１４を送信する。ただし、個人認証情報はPDAに記憶、サービス情報は、ネットワーク経由で入手可能なサービス一覧を用いて、ユーザ０２１０が携帯端末０２１１から選択する。但し、個人認証情報のPDAの記憶に際しては、メモリ及びSIM/WIMカードを用いた記憶方法等を想定している。

２．送信データにPDAの周辺デバイス情報であるIDカード情報（周辺デバイス情報：[info_udev]：{id.udev_001, stat.udev_001, ...}）を加えて電子錠１８１２に送信する。尚、部長１８１０が偶然、課長１８１１のそばを通りかかっ

た場合を回避するために、部長１８１０は明示的にリーダにIDカードをかざす。
３．ユーザ周辺デバイス情報（ユニークなID、状態値等）は共通化された通信プロトコル（BT等）を利用して、PDAが獲得する。
４．PDAからメッセージ（ユーザID、グループID、要求サービスID、ユーザ周辺デバイス情報）１８１４を受信した電子錠１８１２は、機器周辺デバイスである未登録品情報（機器周辺デバイス情報：［info_ddev］：｛id.ddev_001，stat.ddev_001，...｝）を獲得する。尚、不審者１８１３の特定方法については、不審者１８１３の所有する通信機器（IDカード等も含む）への要求に対して、通信そのものは確立されているにも関わらず、応答がない（機器情報を送信しない等）などの場合に対象物を不審者１８１３とみなす方法等も含む。

【００３６】

５．データ（ユーザID、グループID、要求サービスID、ユーザ周辺デバイス情報、機器周辺デバイス情報）と電子錠上のEACLとで照合を行い、アクセスレベルを決定する。
６．決定されたアクセスレベルのモードで電子錠１８１２を制御する。
７．課長１８１１にサービス（金庫を開錠しないというサービス）を提供する。
８．尚、補足として、金庫内に重要物品がある場合セキュリティシステムが作動し、そうでない場合は複数（例えば、登録された全て）のユーザからの入室許可を認める等の実施例も含むことを付記する。

【００３７】

図１９は、本発明におけるアクセス制御方法を適用した実施例２を示す概略図である。主な構成要素として、客１９１０、店員１９１１、商品（CD等）１９１２、店入口１９１３等から構成される。店員１９１１は、携帯端末０２１１として店員カードを所有している。また、ユーザ周辺デバイス０２１８としては、店頭に並ぶタグ付き商品（CD等）を想定している。

【００３８】

さらに、この適用例のサービスデバイス０２２０としては、未精算の商品(CD等)持ち出しをチェックする警報機付きタグリーダを常設した店入口１９１３を考える。具体的には、精算時商品（CD等）に貼付されたタグに精算済み情報を書

き込み、店入口１９１３にてそのタグを読みとる。読み取った情報に精算済み情報が含まれておらず、かつ商品（CD等）を所持している者が店員でない場合警報を鳴らすものである。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『未清算の商品(CD等)１９１２を所持した客１９１０が店入口１９１３に差し掛かると警報機が鳴るが、店員１９１１が商品(CD等)１９１２を所持して店入口を通過しても警報機は鳴らない。』さらに詳述すると、以下のようである。

【００３９】

１．客１９１０が未清算のまま店入口１９１３を通過しようとすると、商品（CD等）タグ（未清算情報を含む）が入口付近に常設されたリーダによって読み取られる。

２．読み取られた情報が、商品の未清算情報である場合、リーダの警報機が作動する。

３．店員１９１０が未清算の商品（CD等）１９１２を所持したまま店入口１９１３を通過しようとした場合は、店員１９１１の所有する店員カード及び商品（CD等）タグ（未清算情報を含む）が入口付近に常設されたリーダによって読み取られる。

４．読み取られた情報が、店員情報である場合商品（CD等）１９１２のタグ情報に書き込まれた精算/未清算情報に依らずリーダの警報機は作動しない。

【００４０】

図２１は、本発明におけるアクセス制御方法を適用した実施例３を示す概略図である。主な構成要素として、社員Ａ２１１０、社員Ｂ２１１１、エレベータ２１１２等から構成される。社員Ａ２１１０及び社員Ｂ２１１１は、携帯端末等を用いてエレベータ２１１２を要求する階に呼び出す。社員Ａは、エレベータ２１１２からある一定の距離（近傍距離閾値）２１１３以上の場所からサービスを要求し、社員Ｂは、近傍距離閾値２１１３を半径とする円内からサービスを要求する。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『エレベータから遠くの場所（近傍距離閾値２１１３以上離れた場所）に居る社員Ａ２１１０はエレベータ２１１

２を呼び出せないが、近く（近傍距離閾値２１１３を半径とする円内領域）に居る社員Ｂはエレベータ２１１２を呼び出すことができる。』さらに詳述すると、以下のようである。

【００４１】

１．社員Ａ２１１０は、携帯端末等を用いてエレベータ２１１２に対してエレベータ呼び出しの要求メッセージを送信する。

２．携帯端末からメッセージが送信された時間とエレベータ２１１２で受信した時間差等を用いて、エレベータと社員Ａの携帯端末等との距離を測定する。但し、距離の測定方法に関しては他の方法でもよい。

３．上記の測定距離が近傍距離閾値１２１３以上の場合、エレベータはアクセスを許可しない。

４．逆に、社員Ｂ１２１１のように、測定距離が近傍距離閾値以下の場合は、エレベータはアクセスを許可し社員Ｂ２１１１に対してサービスを提供する。

【００４２】

図２２は、本発明におけるアクセス制御方法を適用した実施例４のシステムの構成図である。主な構成要素は、社員２２１０、不審者２２１１、社員所有の携帯端末２２１２、不審者所有の携帯端末２２１３、正門２２１４、履歴情報ＤＢ２２１５、持出物２２１６等から構成される。

【００４３】

そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『携帯端末２２１２を所持した社員Ａは正門を通過できるが、携帯端末２２１３を所持しているにも関わらず積極的に個人情報を送信しようとせず、持出物２２１６を持ち出そうとしている不審者２２１１が正門を通過しようとするとチェックがかかる。周辺機器構成と併せて、持出物２２１６の履歴情報ＤＢ２２１５を用いることで、不審者２２１１は正門を通過できない。』さらに詳述すると、以下のようである。

【００４４】

１．携帯端末２２１２を所持した社員Ａ２２１０が正門を通過しようとすると、上記携帯端末２２１２から個人情報を獲得する。

２．社内ＤＢ等の参照を行い、上記社員Ａが社員であることを確認し正門を通過させる。

３．携帯端末２２１３、持出物２２１６を所持する不審者２２１１が正門を通過しようとすると、携帯端末２２１３から個人情報が取り出せない。通信は確立されているが、意図的に個人情報等のデータを送信しないようにしている場合等である。

４．持出物２２１６の履歴情報ＤＢ２２１５を参照する。

５．対象機器２６１１を持出物２２１６、参照開始点２６１２を図書、参照終了点２６１３を正門、履歴情報２６１４を不審者２２１１の行動履歴情報（時刻２５１０、状態（値）２５１１、周辺機器２５１２）としてアクセスレベルを決定する。

６．周辺機器構成を用いて得られるアクセスレベルと上記アクセスレベルを比較して、ある政策（例えば、アクセスレベルの低い方を優先する等）に従ってアクセスレベルを決定する。

７．決定されたアクセスレベルに従ってアクセス制御を行う。

【００４５】

図２５は、本発明におけるユーザ／機器の履歴情報データベースの構成図である。主な構成要素として、時刻２５１０、状態（値）２５１１、周辺機器２５１２等から構成される。時刻２５１０は、ある対象となるユーザ／機器の履歴情報を採取した時刻（日付情報等含む）である。状態（値）２５１１は、時刻２５１０における対象ユーザ／機器の状態値である。例えば、対象が図書の書籍であるような場合は、「貸出未申請」「貸出既申請」等である。周辺機器２５１２は、時刻２５１０、状態（値）２５１１時における対象物ユーザ／機器の周辺に存在する機器である。

【００４６】

図２６は、本発明における履歴情報データベースを用いた場合のEACLを示す図である。主な構成要素として、アクセスレベル２６１０、対象機器２６１１、参照開始点２６１２、参照終了点２６１３、履歴情報２６１４等から構成される。アクセスレベル２６１０は、本EACLにおいて決定される対象機器２６１１のアク

セスレベルである。参照開始点２６１２は、である。参照終了点２６１３は、である。履歴情報２６１４は、対象機器２６１１の参照開始点２６１２から参照終了点２６１３間における、ある対象者の行動履歴情報（状態（値）２５１０、時刻２５１１、周辺機器２５１２）ある。

【００４７】

図２４は、本発明におけるアクセス制御方法を適用した実施例５のシステム構成図である。主な構成要素は、午前にサービスを要求する社員Ａ２４１０、午後にサービスを要求する社員Ａ２４１１、部屋のドア２４１２等から構成される。そこで、本発明における周辺デバイス情報を用いたアクセス制御システムの適用例における概略は以下に示す通りである。『社員Ａ２４１０及び２４１１は、午前中に申請すれば部屋に入ることができるが、午後に申請すると入れない。』さらに詳述すると、以下のようである。

【００４８】

１．午前中に社員Ａ２４１０が部屋への入室許可申請メッセージを送信する。
２．上記メッセージは、上記実施例１乃至４と同様に周辺機器構成、周辺機器状態等を含んでいる。
３．社員Ａ２４１０が午前中に申請を行った場合、部屋への入室が許可される。
４．社員Ａ２４１１が午後から申請を行った場合、
上記周辺機器情報等が同一でも、部屋への入室は許可されない。
５．また、社員Ａ２４１０及び２４１１が申請を行った時間に関わらず、サービス提供時の時間（帯）（部屋の利用時間等）によって入室許可を発行するとう実施例も含む。

【００４９】

図２０は、本発明におけるアクセス制御方法を適用した実施例６のシステムの構成図である。主な構成要素として、サービス要求デバイス２０１０、アクセスレベル認証局２０１２、サービス配信デバイス２０１３等から構成される。サービス要求デバイスは、サービス配信デバイス２０１３に対してサービス要求を送信する。この場合、ユーザ２０１０及びユーザ周辺デバイス０２１８の情報とともにサービス要求を送信する。上記要求を受信したサービス配信デバイス２０１

３は、アクセスレベル照会処理２０１４を用いてアクセス認証局２０１２にアクセスレベルの照会を行う。その際、サービス要求デバイス２０１０から受信した情報及び機器周辺デバイス０２２８情報を送信する。上記情報を受信したアクセスレベル認証局２０１２は、EACLを用いてアクセスレベルを決定し、サービス配信デバイス２０１３に送信する。上記アクセスレベル情報を受信したサービス配信デバイス２０１３は、受信したアクセスレベルに応じたサービスを提供する。本構成を用いたシステムにおける実施例は、上記実施例１乃至５に該当する。

【００５０】

上述した実施例は、以上詳述したように構成されており、次のような効果を奏する。（１）サービス受信側と送信側の周辺状態を含めた木目の細かいアクセス制御が可能となる。（２）ユーザ/サービスデバイスの周辺状態の変更に対して柔軟なアクセス制御が可能となる。

【００５１】

【発明の効果】

本発明によれば、アクセス制御などのサービス提供を、きめ細かく実行することが可能になる。

【図面の簡単な説明】

【図１】本発明におけるアクセス制御システムの適用形態例を示した図である。

【図２】本発明におけるアクセス制御システムの構成図である。

【図３】本発明におけるシステム全体の処理を示すフローチャートである。

【図４】本発明における携帯端末上の周辺デバイス検出処理を示すフローチャートである。

【図５】本発明における携帯端末上の機器構成管理処理を示すフローチャートである（非常駐処理）。

【図６】本発明における携帯端末上の機器構成管理処理を示すフローチャートである（常駐処理）。

【図７】本発明におけるサービスデバイス上の周辺デバイス検出処理を示すフローチャートである。

【図８】本発明におけるサービスデバイス上の機器構成管理処理を示すフローチ

ャートである（非常駐処理）。

【図９】本発明におけるサービスデバイス上の機器構成管理処理を示すフローチャートである（常駐処理）。

【図１０】本発明においてユーザが携帯端末を介してサービスを要求する際に送信するメッセージを示した図である。

【図１１】本発明におけるユーザから送信の情報を示す図である。

【図１２】本発明におけるユーザ周辺デバイス情報を示す図である。

【図１３】本発明における周辺デバイス情報を利用したEACLを示す図である。

【図１４】本発明におけるアクセスレベルと実行許可処理との関係を示す図である。

【図１５】本発明における周辺デバイスの判定基準を示す図である。

【図１６】本発明における周辺閾値（近傍距離閾値）の既定方法を示す図である。

【図１７】本発明におけるサービスによる異なる周辺距離の例を示す概略図である。

【図１８】本発明におけるアクセス制御方法を適用した実施例１を示す概略図である。

【図１９】本発明におけるアクセス制御方法を適用した実施例２を示す概略図である。

【図２０】本発明におけるアクセス制御方法を適用した実施例６のシステムの構成図である。

【図２１】本発明におけるアクセス制御方法を適用した実施例３のシステム構成図である。

【図２２】本発明におけるアクセス制御方法を適用した実施例４のシステム構成図である。

【図２３】本発明におけるサービス要求／提供時の時間（帯）によってアクセスレベルが変化するEACLを示す図である。

【図２４】本発明におけるアクセス制御方法を適用した実施例５のシステム構成図である。

【図２５】本発明におけるユーザ／機器の履歴情報データベースの構成図である。

【図２６】本発明における履歴情報データベースを用いた場合のEACLを示す図である。

【図２７】本発明における履歴情報データベースを用いた場合のシステム全体の処理を示すフローチャートである。

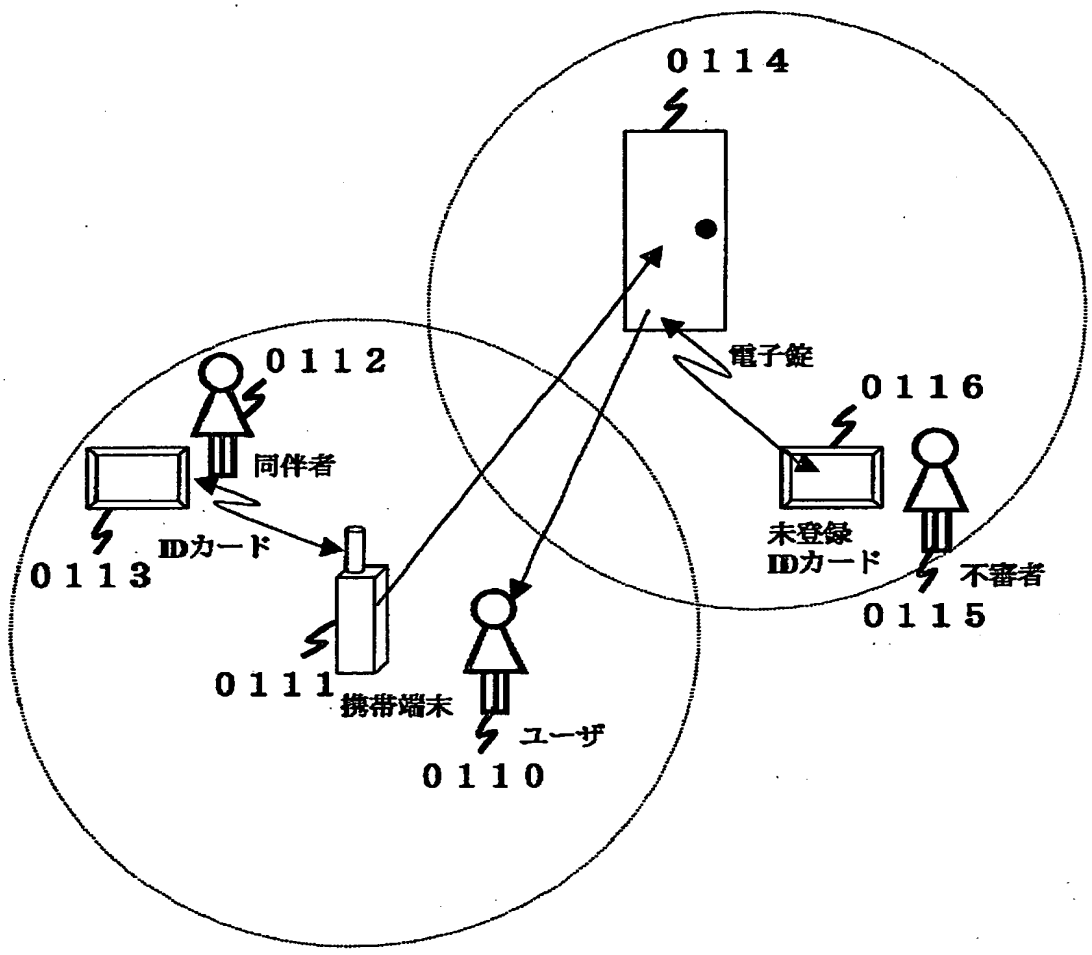
【符号の説明】

０２１０…システムサービスの対象となるユーザ、０２１１…携帯端末、０２１２…携帯端末のI／O、０２１３…アプリケーションプログラム、０２１４…データベース、０２１８…周辺デバイス、０２２０…サービスデバイス、０２２１…アプリケーションプログラム、０２２３…EACLのファイル本体、０２２６…データベース、０２２８…周辺デバイス。

【書類名】　図面

【図１】

図１



出証特２００１－３１０２４００

【図２】

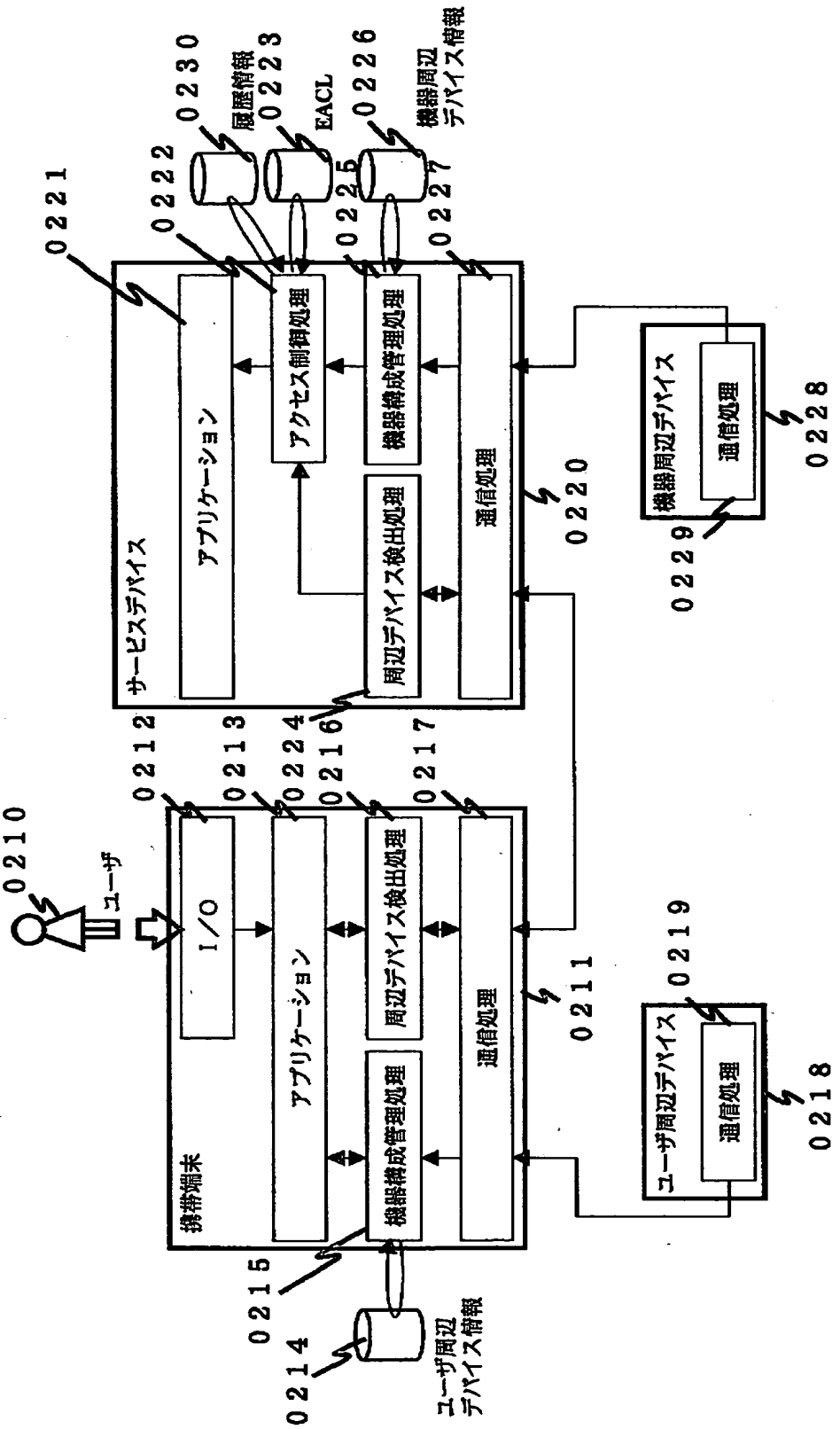
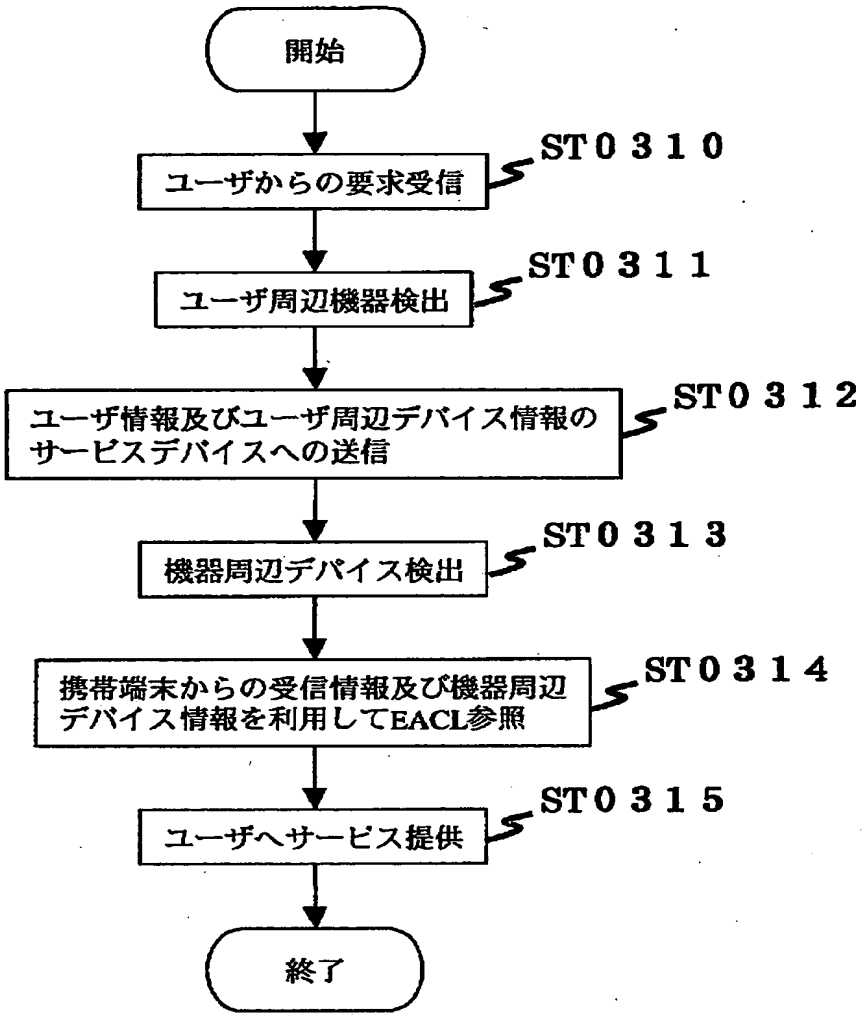

0230
履歴情報
0223
EACL
0226
機器周辺
デバイス情報
0222
0225
0227
0221
アクセス制御処理
機器構成管理処理
アプリケーション
サービスデバイス
周辺デバイス検出処理
通信処理
0220
0229
機器周辺デバイス
通信処理
0228
0212
0213
0224
0216
0217
0210
ユーザ
I/O
アプリケーション
周辺デバイス検出処理
携帯端末
機器構成管理処理
通信処理
0211
0219
ユーザ周辺デバイス
通信処理
0218
0215
0214
ユーザ周辺
デバイス情報

図2

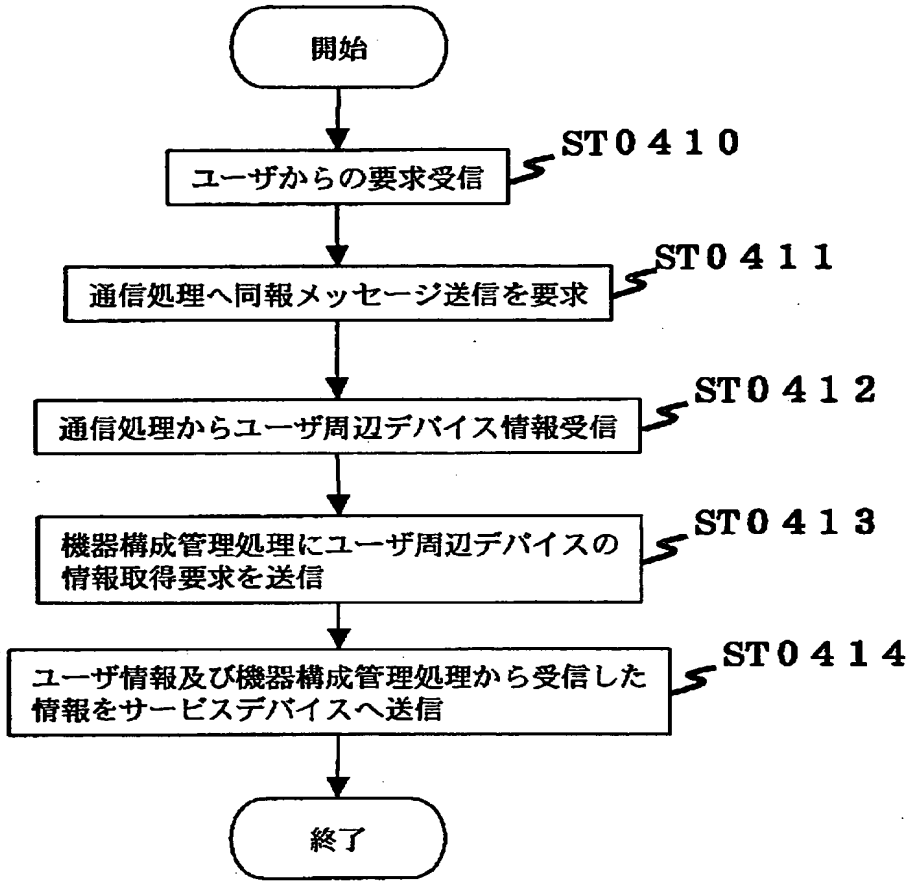
【図３】

図３


開始
ユーザからの要求受信
ST０３１０
ユーザ周辺機器検出
ST０３１１
ユーザ情報及びユーザ周辺デバイス情報のサービスデバイスへの送信
ST０３１２
機器周辺デバイス検出
ST０３１３
携帯端末からの受信情報及び機器周辺デバイス情報を利用してEACL参照
ST０３１４
ユーザへサービス提供
ST０３１５
終了

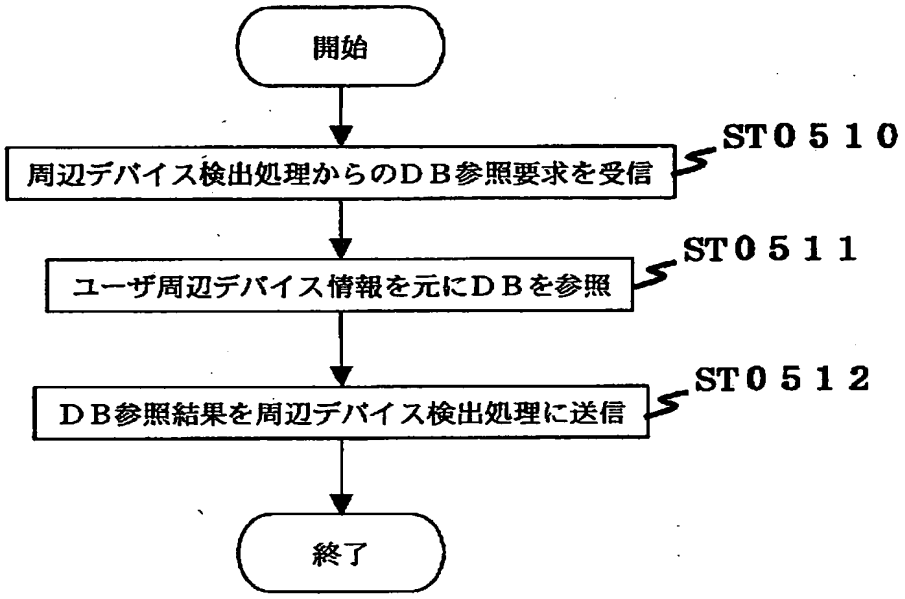
【図４】

図４


開始
ユーザからの要求受信
ST０４１０
通信処理へ同報メッセージ送信を要求
ST０４１１
通信処理からユーザ周辺デバイス情報受信
ST０４１２
機器構成管理処理にユーザ周辺デバイスの情報取得要求を送信
ST０４１３
ユーザ情報及び機器構成管理処理から受信した情報をサービスデバイスへ送信
ST０４１４
終了

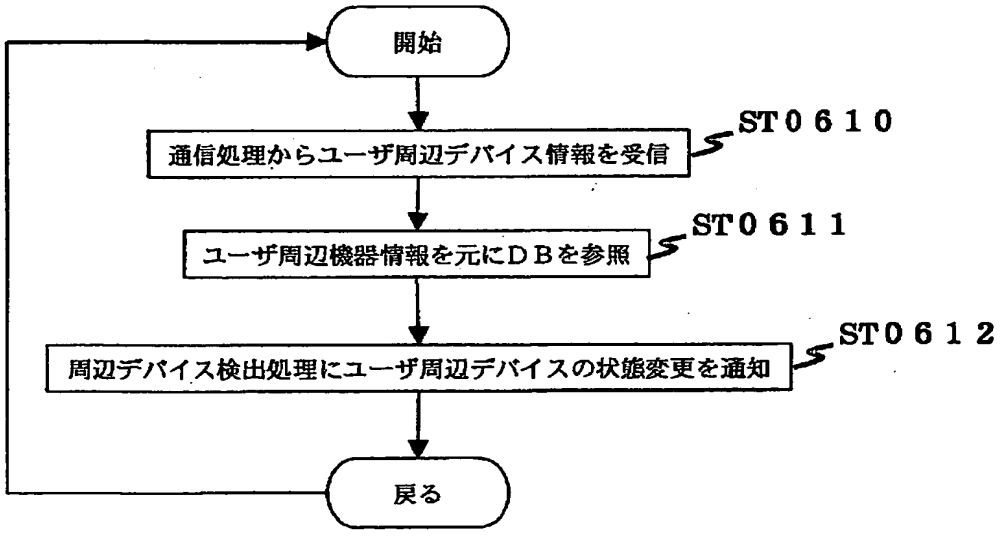
【図５】

図５


開始
周辺デバイス検出処理からのＤＢ参照要求を受信
ST０５１０
ユーザ周辺デバイス情報を元にＤＢを参照
ST０５１１
ＤＢ参照結果を周辺デバイス検出処理に送信
ST０５１２
終了

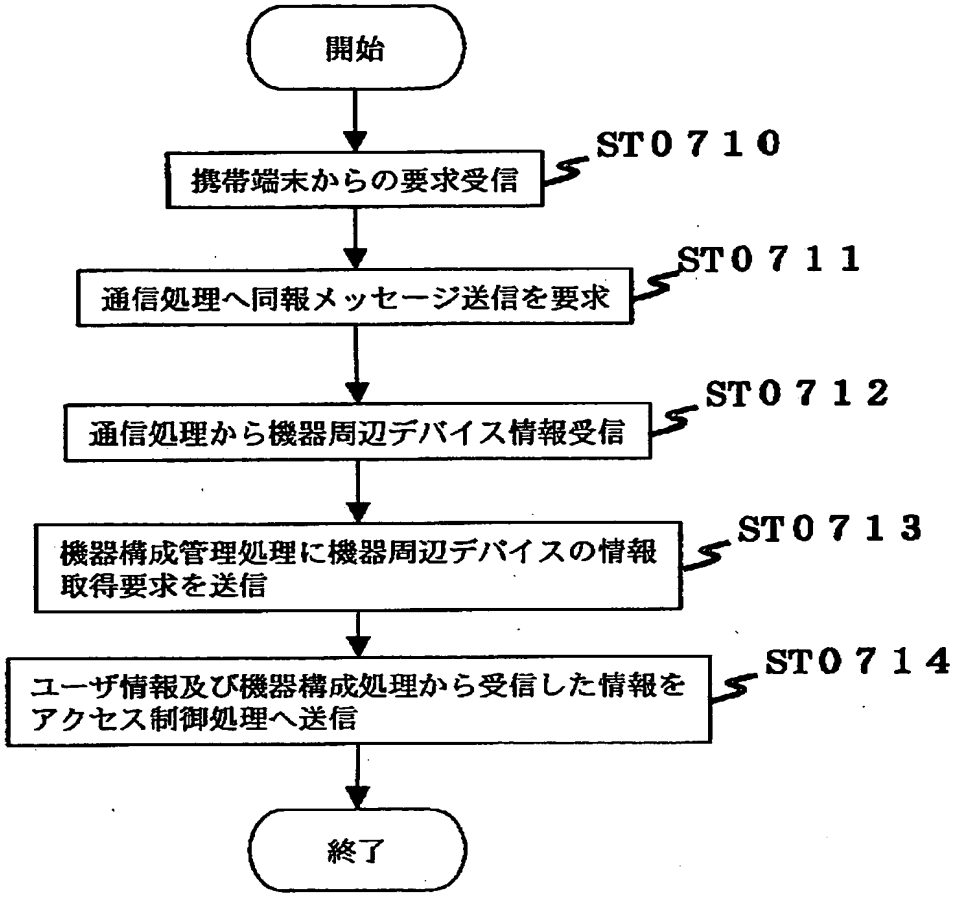
【図６】

図６


開始
通信処理からユーザ周辺デバイス情報を受信
ST０６１０
ユーザ周辺機器情報を元にＤＢを参照
ST０６１１
周辺デバイス検出処理にユーザ周辺デバイスの状態変更を通知
ST０６１２
戻る

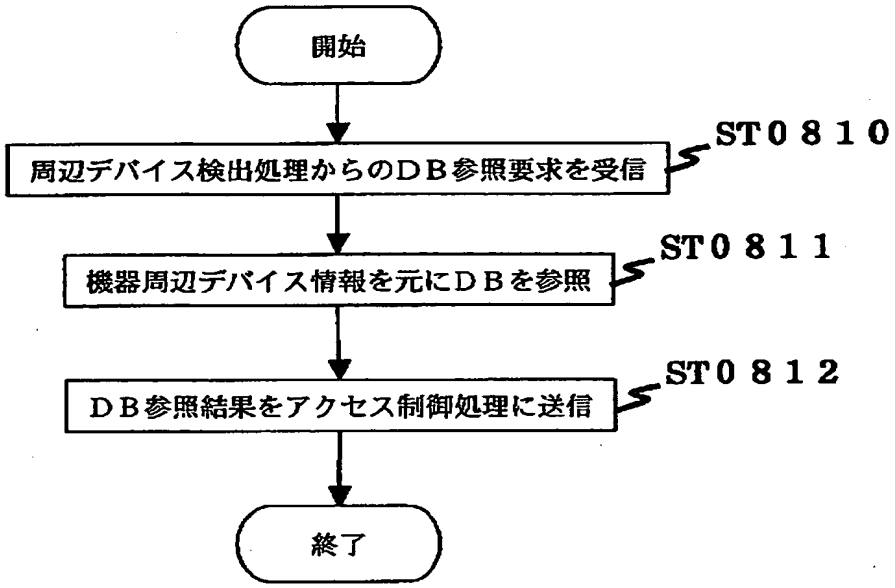
【図７】

図７


開始
携帯端末からの要求受信
ST０７１０
通信処理へ同報メッセージ送信を要求
ST０７１１
通信処理から機器周辺デバイス情報受信
ST０７１２
機器構成管理処理に機器周辺デバイスの情報取得要求を送信
ST０７１３
ユーザ情報及び機器構成処理から受信した情報をアクセス制御処理へ送信
ST０７１４
終了

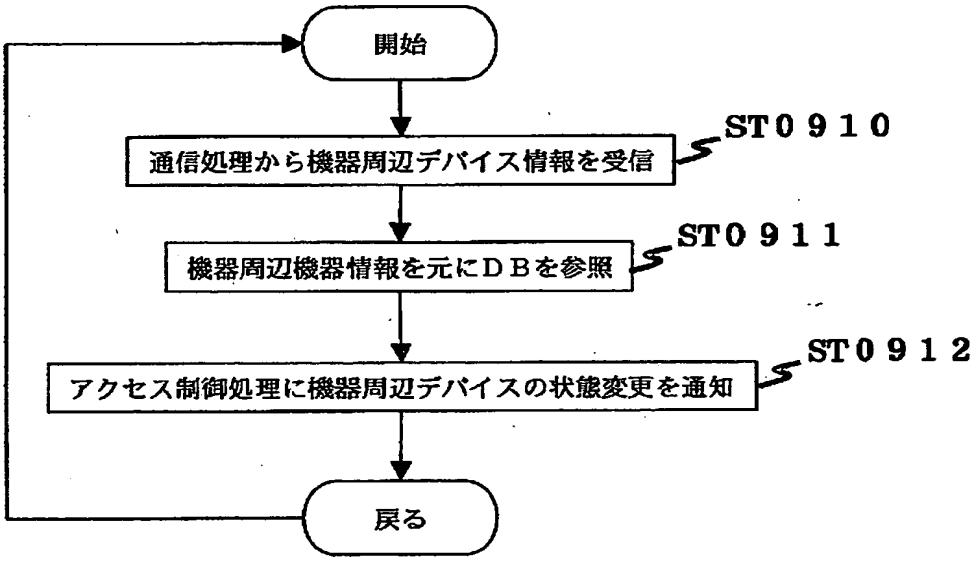
【図８】

図８


開始
周辺デバイス検出処理からのＤＢ参照要求を受信
ST０８１０
機器周辺デバイス情報を元にＤＢを参照
ST０８１１
ＤＢ参照結果をアクセス制御処理に送信
ST０８１２
終了

【図９】

図９


開始
通信処理から機器周辺デバイス情報を受信
ST０９１０
機器周辺機器情報を元にＤＢを参照
ST０９１１
アクセス制御処理に機器周辺デバイスの状態変更を通知
ST０９１２
戻る

【図１０】

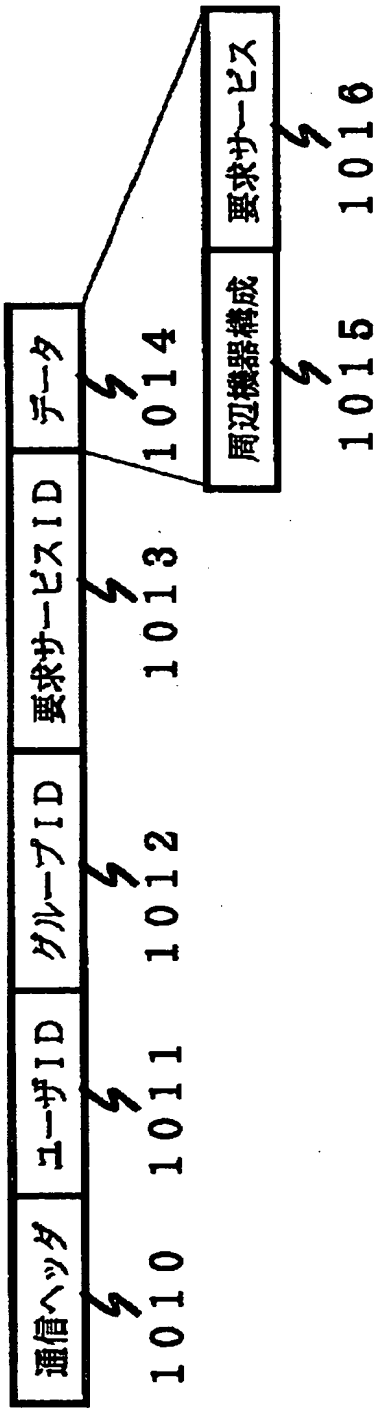

通信ヘッダ
ユーザＩＤ
グループＩＤ
要求サービスＩＤ
データ
周辺機器構成
要求サービス
1010
1011
1012
1013
1014
1015
1016

図１０

【図１１】

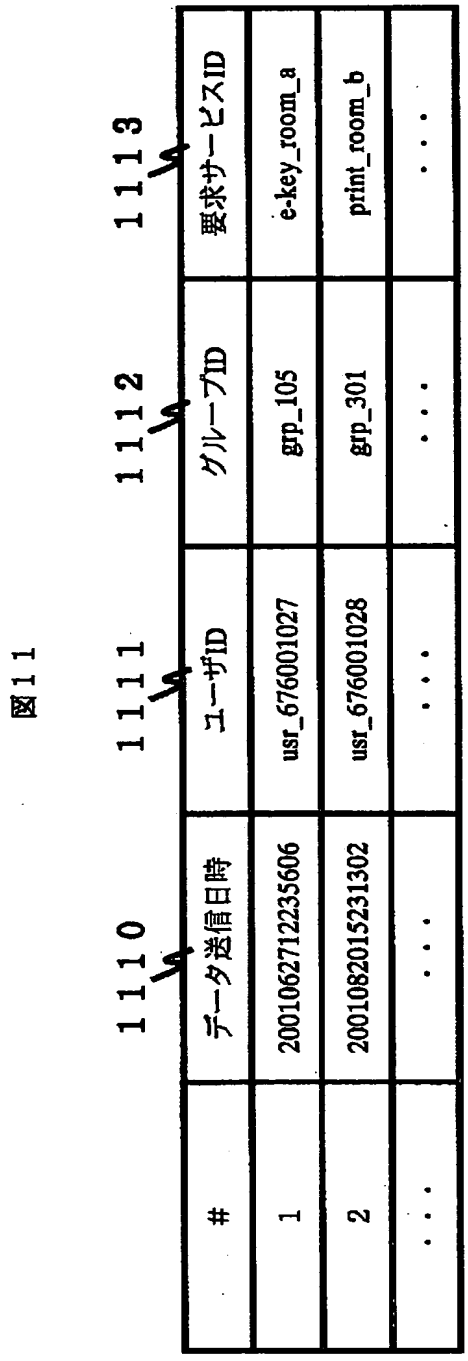

1110
1111
1112
1113
#
データ送信日時
ユーザID
グループID
要求サービスID
1
2001062712235606
usr_676001027
grp_105
e-key_room_a
2
2001082015231302
usr_676001028
grp_301
print_room_b

図１１

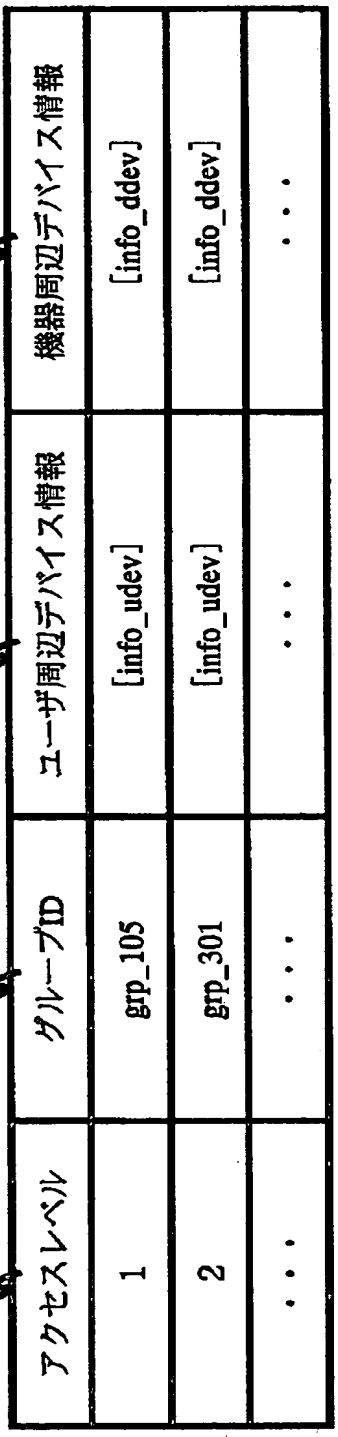
【図１２】

図１２

	１２１０	１２１１
#	データ受信日時	ユーザ周辺デバイス情報
1	2001062712235606	[info_udev]
2	2001082015231302	[info_udev]
・・・	・・・	・・・

【図１３】

図１３


1310
1311
1312
1313
アクセスレベル
グループID
ユーザ周辺デバイス情報
機器周辺デバイス情報
1
grp_105
[info_udev]
[info_ddev]
2
grp_301
[info_udev]
[info_ddev]
・・・
・・・
・・・
・・・

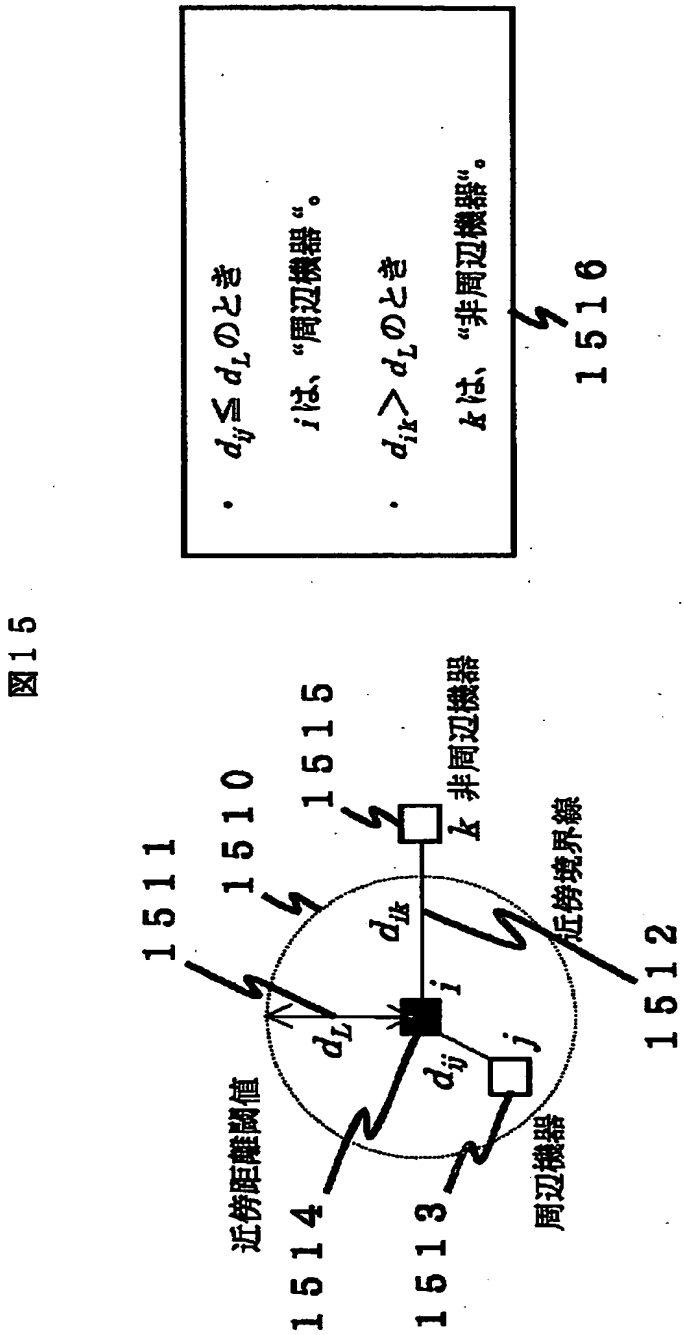
【図１４】

図１４

1410 アクセスレベル	1411 実行処理	1412 アクセス権限
0	処理１	×
	処理２	×
	処理３	×
	・・・	・・・
1	処理１	×
	処理２	○
	処理３	×
	・・・	・・・
・・・	・・・	・・・

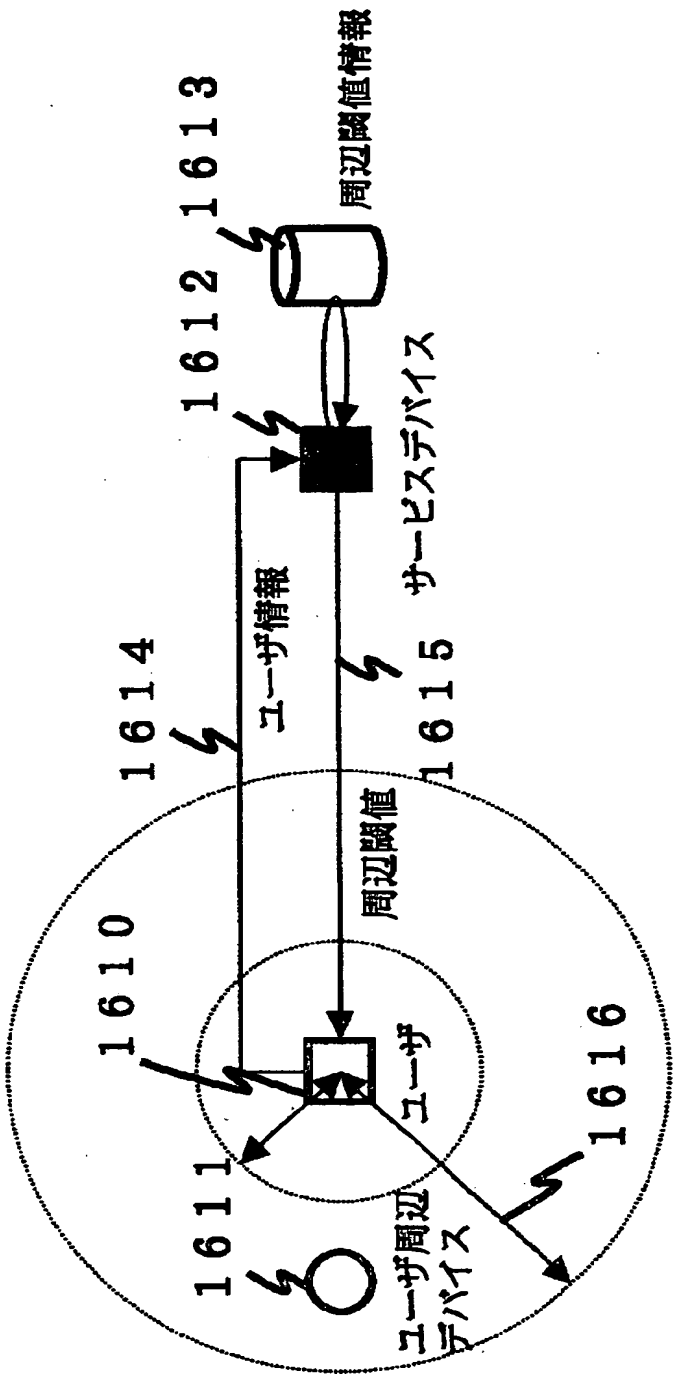
【図１５】

図１５


・ $d_{ij} \leq d_L$ のとき
i は、“周辺機器“。
・ $d_{ik} > d_L$ のとき
k は、“非周辺機器“。
1516
1511
1510
1515
k 非周辺機器
近傍境界線
1512
d_{ik}
i
d_L
d_{ij}
j
近傍距離閾値
周辺機器
1514
1513

【図１６】

図16


周辺閾値情報
1613
1612
サービスデバイス
ユーザ情報
1614
1615
周辺閾値
1610
ユーザ
1616
1611
ユーザ周辺
デバイス

【図１７】

図１７

#	サービス (1710)	周辺距離[m] (1711)
1	ドアの開錠	１０
2	ドアの施錠	0
・・・	・・・	・・・

【図１８】

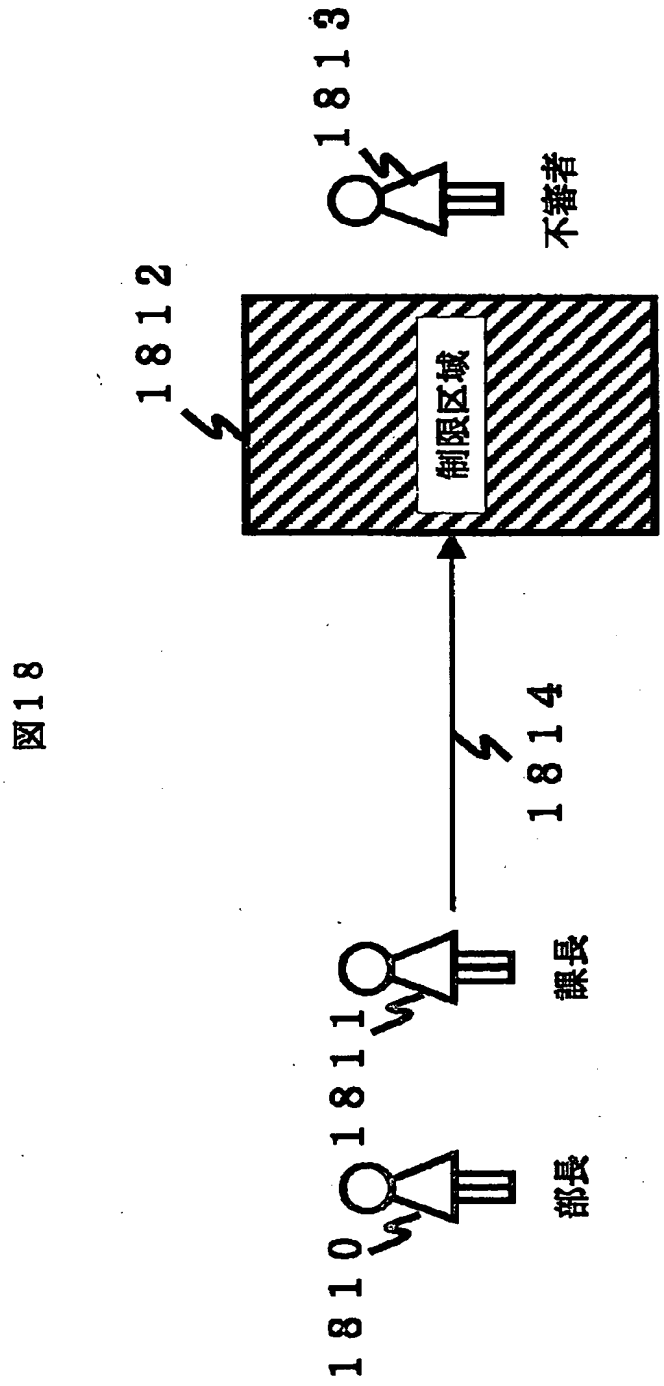


図18

【図１９】

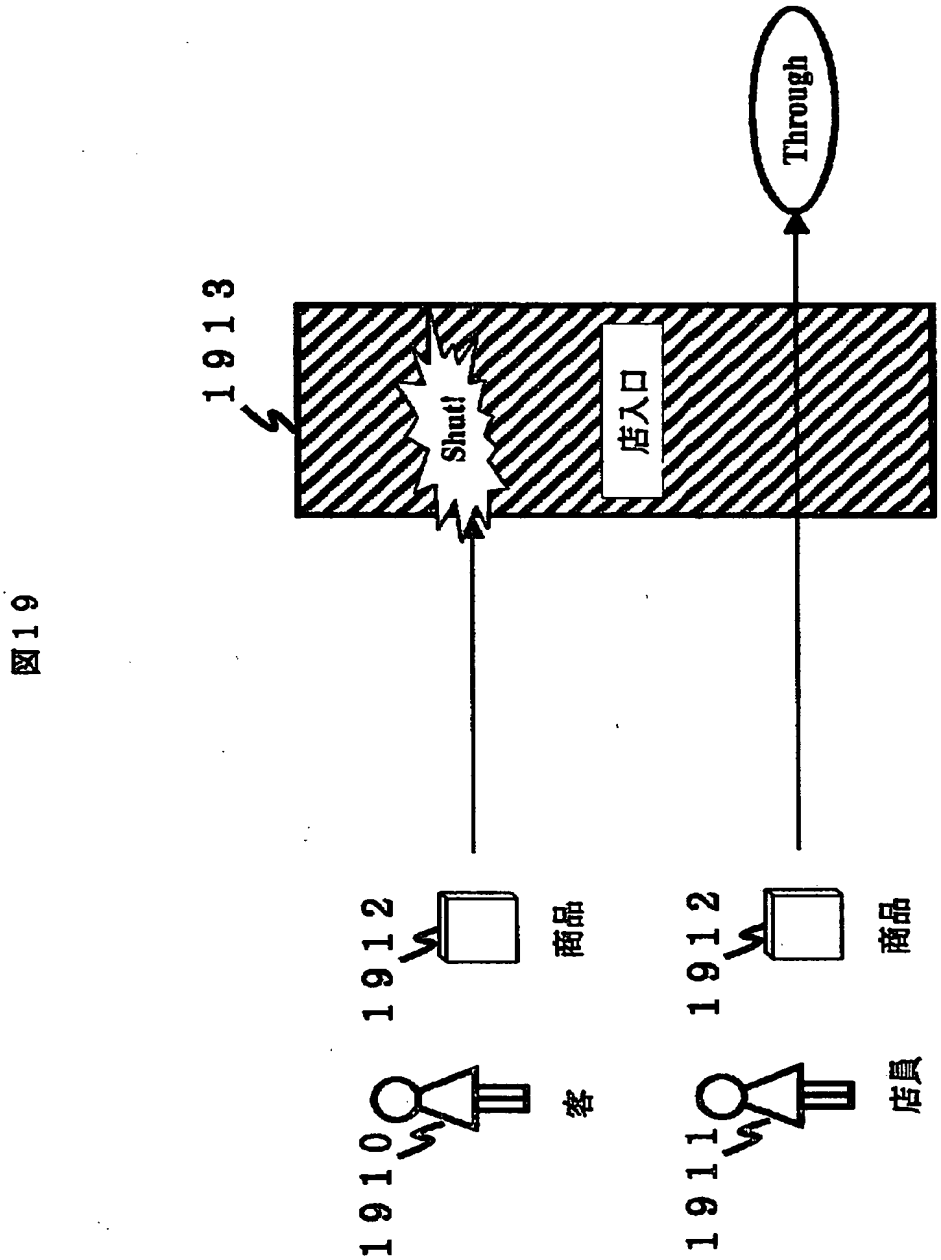
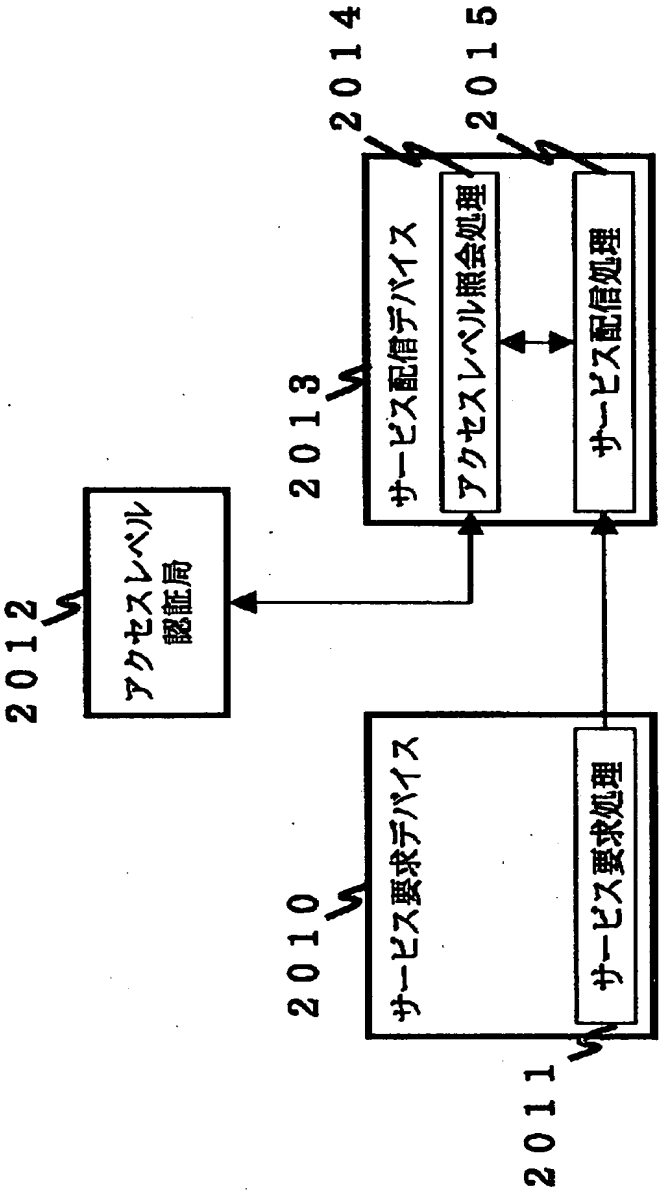


図19

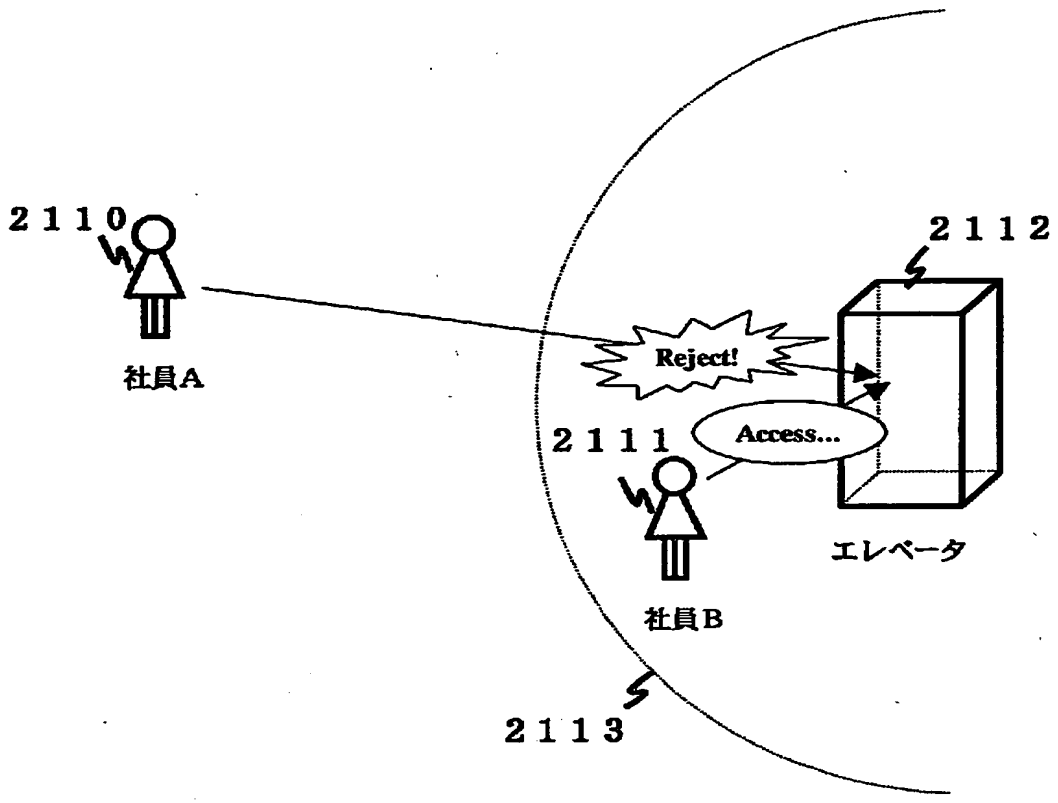
【図２０】

図２０


2014
2015
2013
サービス配信デバイス
アクセスレベル照会処理
サービス配信処理
2012
アクセスレベル認証局
2010
サービス要求デバイス
サービス要求処理
2011

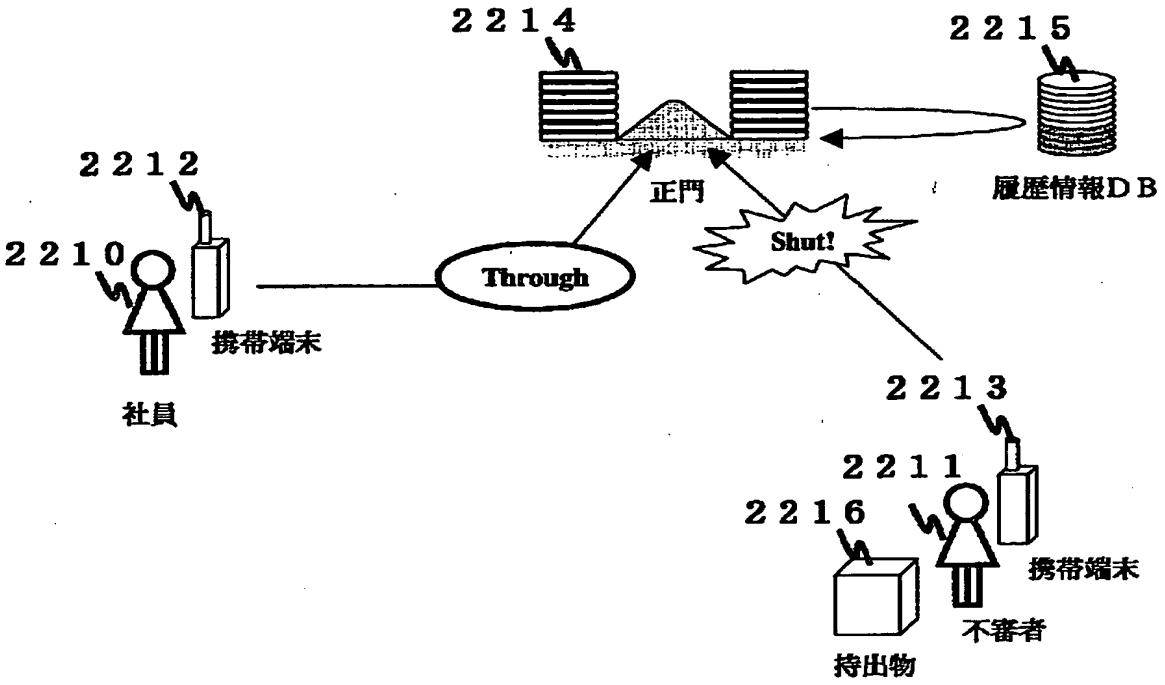
【図２１】

図２１



【図２２】

図２２



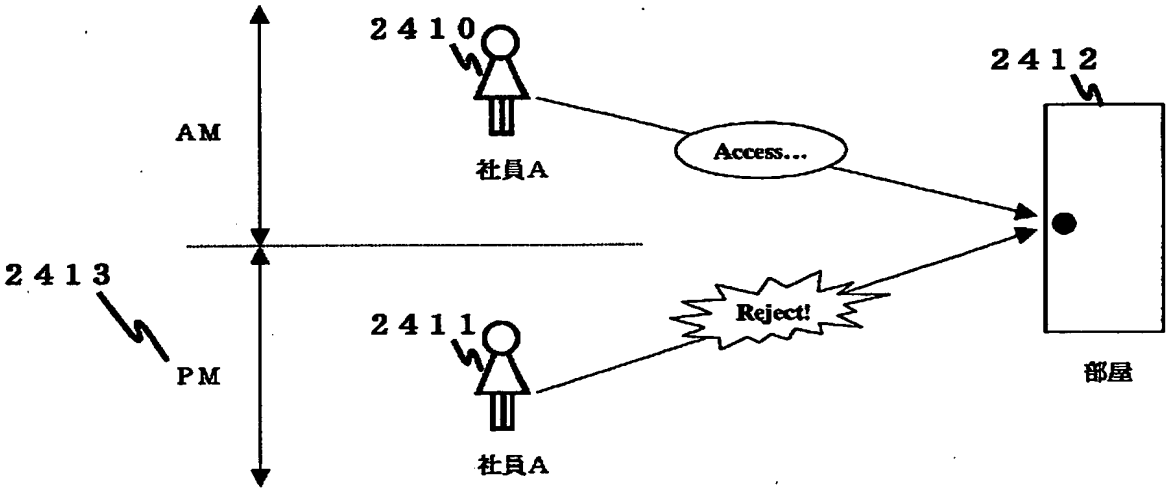
【図２３】

図２３

２３１０ 受信情報	２３１１ 時間（帯）	２３１２ アクセスレベル
inf_receive	AM	1
inf_receive	PM	2
・・・	・・・	・・・

【図２４】

図２４



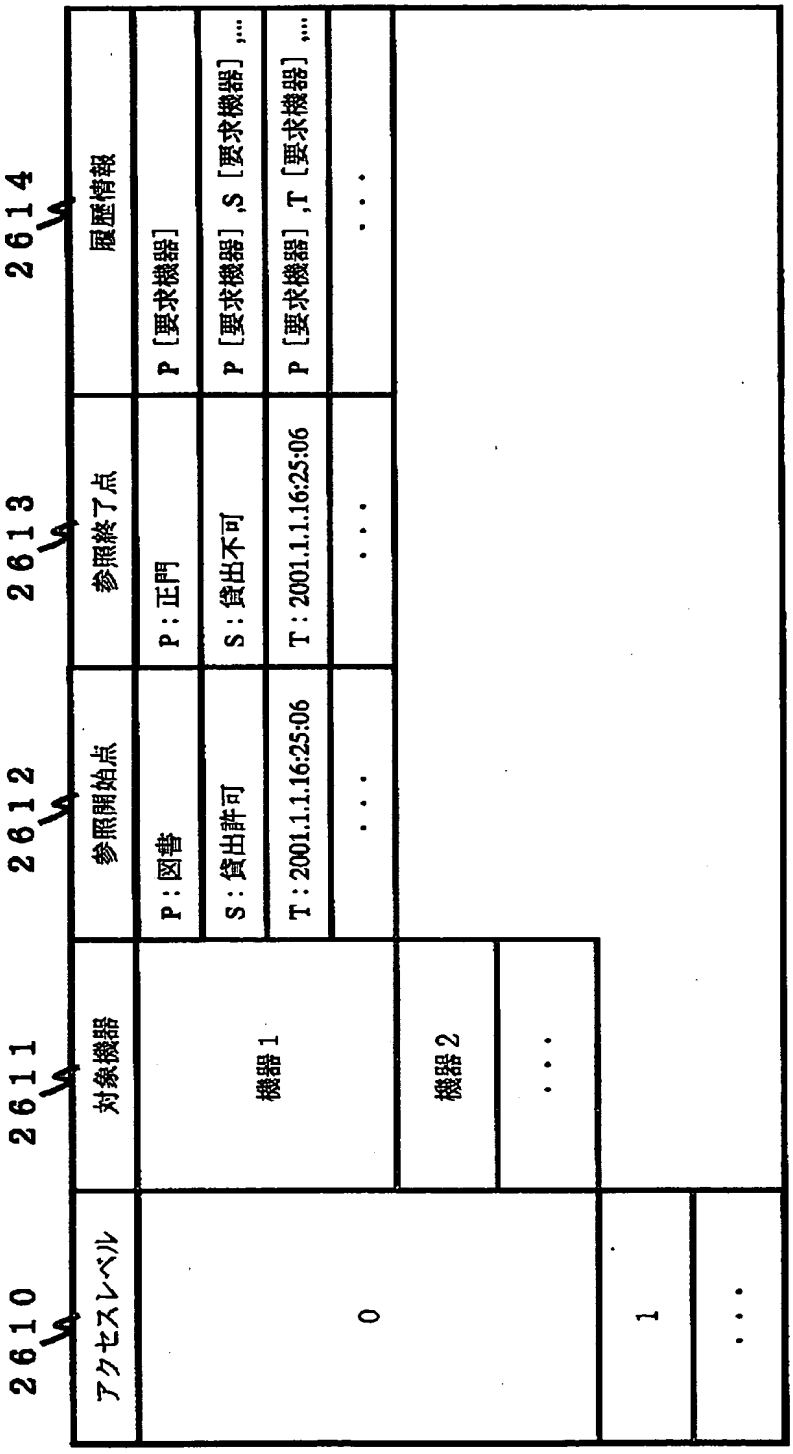
【図２５】

図２５

２５１０ #	２５１１ 時刻	２５１２ 状態（値）	周辺機器
1	2001.1.1.16:25:06	ON	PC_2L, ELV_2L, ...
2	2001.1.2.12:55:26	OFF	PC_1L, ELV_1L, ...
・・・	・・・	・・・	・・・

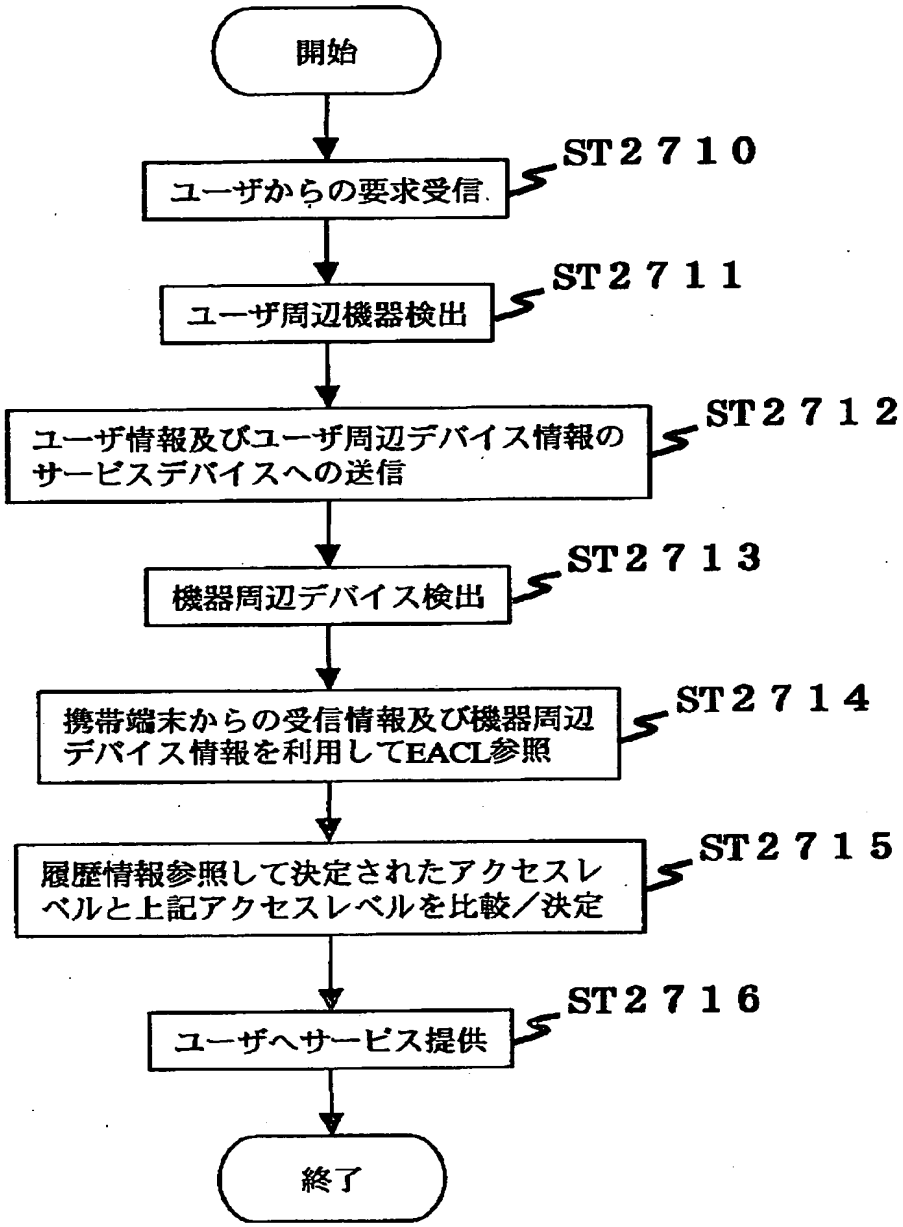
【図２６】

図２６


2610
2611
2612
2613
2614
アクセスレベル
対象機器
参照開始点
参照終了点
履歴情報
0
機器１
P：図書
S：貸出許可
T：2001.1.1.16:25:06
P：正門
S：貸出不可
T：2001.1.1.16:25:06
P［要求機器］
P［要求機器］,S［要求機器］,…
P［要求機器］,T［要求機器］,…
機器２
1
…

【図２７】

図２７


開始
ユーザからの要求受信
ST２７１０
ユーザ周辺機器検出
ST２７１１
ユーザ情報及びユーザ周辺デバイス情報のサービスデバイスへの送信
ST２７１２
機器周辺デバイス検出
ST２７１３
携帯端末からの受信情報及び機器周辺デバイス情報を利用してEACL参照
ST２７１４
履歴情報参照して決定されたアクセスレベルと上記アクセスレベルを比較／決定
ST２７１５
ユーザへサービス提供
ST２７１６
終了

【書類名】　要約書

【要約】

【課題】

従来においては、様々なユーザが訪問するオフィスビル等において、制限区域内に重要物が存在する場合には入室を禁止し、そうでない場合は許可するような場面を想定した時、従来の画一的なアクセス制御では運用/管理者のアクセスレベルの設定変更作業やユーザの設定変更要求からの時間的な遅れという点で限界があった。

【解決手段】

（１）ユーザ（デバイスにアクセスする人）及びサービスデバイス（ユーザにアクセスされるデバイス）の周辺機器情報を収集する手段を有する。（２）サービスデバイスへのアクセスを許可するか、しないかを判断する手段を有する。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２００１－１７４９８１
受付番号	５０１００８３４３２３
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１３年　６月１２日

＜認定情報・付加情報＞

【提出日】　平成13年 6月11日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所